PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

PCT/FI99/01010

Helsinki 13.01.2000

09/868107

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT

Hakija Applicant	**Nokia Telecommunications Oy** **Espoo**
Patenttihakemus nro Patent application no	**982727**
Tekemispäivä Filing date	**16.12.1998**
Kansainvälinen luokka International class	**H04Q**

Keksinnön nimitys
Title of invention

"A method for controlling connections to a mobile station"

Hakijan nimi on hakemusdiaariin **05.12.1999** tehdyn nimenmuutoksen jälkeen **Nokia Networks Oy**.

The application has according to an entry made in the register of patent applications on **05.12.1999** with the name changed into **Nokia Networks Oy**.

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A
P.O.Box 1160
FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5204
Telefax: + 358 9 6939 5204

A method for controlling connections to a mobile station

TECHNICAL FIELD OF THE INVENTION

The present invention relates to communication networks capable of ciphering and deciphering and especially to a method for managing keys.

BACKGROUND OF THE INVENTION

Radio transmission is by nature more prone to eavesdropping and fraud than fixed wire transmission. Listening to communications is easy and does not require access to special locations. The GSM cellular system has alleviated this problem by introducing authentication and encryption or ciphering. Next the GSM authentication and ciphering procedures are explained shortly in reference with Figure 1. More details can be found for example in Mouly et. al.: "The GSM system for mobile communications".

Figure 1 illustrates current GSM system incorporated with a general packet radio or GPRS network. The complete network comprises three different functional sub-networks. Radio access network comprises Base Station Controllers or BSC's 30 (only one is shown) and Base Stations or BS's 20. The first core network comprises Mobile Switching Center with Home Location Register or MSC/VLR 40 and a Home Location Register with Authentication Center or HLR/AuC 50. The first core network comprises additional MSC/VLR's and HLR/AuC's, which are not shown for the sake of simplicity. The second core network is a packet network and comprises Serving General packet Service Node or SGSN 60. The second core network comprises additional General packet Service Nodes or GSN's, which are not shown for the sake of simplicity.

When a mobile 10 accesses the first core network it registers itself in the MSC/VLR 40. After receiving the registration request or a service request from the mobile, the MSC/VLR 40 transmits to HLR/AuC a request including IMSI to aqcuire authentication triplets consisting of RAND, SRES and Kc. In GSM it is the MM or the mobility management protocol that implements the functionality for the authentication. Also, the control of the ciphering, ie. the ability to turn ciphering on and off, is at MM level. The triplets are of a predetermined length and calculated by using a secret key Ki, known only to the authentication center. After receiving the triplets from HLR/AuC the MSC/VLR sends the challenge, RAND, to the MS in an authentication request to authenticate the MS. As part of the succesful registration, the MSC/VLR updates the location of the MS to HLR and downloads the subscriber data from HLR.

The mobile 10 has a secret key Ki in it's SIM card. The secret key Ki is stored on subscription by the operator and is not visible for the users of the mobile or for any other party for that matter. It is identical to the secret key Ki stored in the Authentication Center 50. The secret key Ki is applied together with the random number RAND into a predetermined algorithm called A3 to produce a signed response SRES. The mobile 10 then transmits a message containing SRES to the MSC/VLR 40, which compares it with the SRES received from the AuC 50. If the comparison is succesful, the mobile 10 is authenticated and allowed to access the network. At the same time with calculating the SRES, the mobile and the AuC apply RAND and Ki to another predetermined algorithm called A8 to produce a ciphering key Kc1. If the authentication was succesful and the network so decides, all subsequent transmissions with the mobile 10 over the air interface are ciphered. For this the MSC/VLR transmits the ciphering key Kc1 to that of the BSCs which is in communication with the mobile 10, and the BSC subsequently deliveres the Kc further to the BTS communicating with the MS and the ciphering or

encryption takes place in the base station and the mobile according to yet another predetermined algorithm, for example A5.

If the mobile wants to access the second core network it registers itself in the SGSN 60. The procedure for authentication is similar to the procedure with the first core network, with the exception that the ciphering key Kc2 is not transmitted to the base station (BSS part of the system) currently in communication with the mobile 10. In other words, the ciphering is in SGSN and in MS. The SGSN 60 retains the ciphering key Kc2 within itself and performs the ciphering.

Thus, the prior art system uses different ciphering keys for ciphering the communications with two different core networks and the ciphering is applied to two different radio connections as the radio channels used communications with MSC and SGSN are distinct. As a result, a GSM MS having simultaneous communications with both MSC and SGSN utilizes two ciphering keys to two different radio channels or connections having both their own independent control in the network.

The fact that the ciphering and the control of the ciphering takes place at different locations, may cause consistency problems and the fact that radio access network is not able to access the signalling messages of the second core network at all may turn out to be problematic in future networks when all radio recources used by a specific user should be managed in conjunction in a system having two CN nodes controlling the ciphering. In this case, the radio resources reserved for simultanous connections to MSC and SGSN should be managed by a single entity in the radio access network part of the system, but still there are two entities controlling the ciphering.

However, in proposed that in UMTS there will be only one RRC or radio resouce control protocol, controlling both the connection to the MSC and to the SGSN. If only one key used at a time, the problem is, how to communicate the SGSN that its key is not going to be used. Yet another problem, relates relates to handovers controlled by a CN entity.

It is therefore an object of the present invention to efficiently manage the ciphering keys and algorithms for ciphering and deciphering user data communicated between different core networks and one mobile station.

It is another object of the present invention to efficiently manage the ciphering keys and algorithms for ciphering and deciphering signalling data communicated between different core networks and one mobile station.

It is still another object of the present invention to efficiently transfer the ciphering parameters when the serving radio network controller is handed over to another radio network controller, which then becomes a new serving radio network controller.

SUMMARY OF THE INVENTION

The present invention is a novel and improved method for managing the ciphering keys and algorithms used for encrypting or ciphering the communications of a specific mobile station with multiple core networks or core network entities in a single location. Futher another aspect of the invention is that the management location is movable as the mobile station moves within the radio access network.

The preferred embodiment of the present invention relates to a 3rd generation mobile network, for which abbreviations UMTS or WCDMA are used. The

network is shown in Fig. 2. The network comprises multiple subnetworks. The radio access network or UTRAN (UMTS Terrestial Radio Access Network) comprises multiple Radio Network Controllers or RNC's 130 each of which controls multiple Base Stations or BS's 120. The first core network comprises a Mobile Switching Center with Visitor Location Register or MSC/VLR 140 and a Home Location Register with an Authentication Center or HLR/AuC 150. The first core network comprises additional MSC/VLR's and HLR/AuC's, which are not shown for the sake of simplicity. The second core network is a packet network and comprises Serving General packet Service Node or SGSN 160. The second core network comprises additional General packet Service Nodes or GSN's, which are not shown for the sake of simplicity. Note that the UTRAN may be connected to another operators core network or a third core network similar to the first core network.

Since the air interface access method is CDMA, the mobile 110 is capable of communicating vith multiple base stations at the same time (called soft or diversity handover). When that occurs, all transmissions from the mobile 110 are directed to one RNC, called serving RNC or SRNC, in which the transmissions are combined into one transmission for further sending towards the intended core network.

In the preferred embodiment a mobile station establishes communication with one core network or core network entity or vice versa. In the establishment the network requests mobile to authenticate itself as explained above. At the same time with the authentication the mobile and the network (or CN node) calculate identical ciphering keys Kc1. In the preferred embodiment of the invention the core network or core network entity which calculated the ciphering key does not start ciphering user data or signalling messages but generates and transmits a message comprising the key and data indicative of the algorithm to be used to a ciphering controller 180, which is preferredly

located in the serving radio network controller. The ciphering controller receives said message and starts ciphering the data and signalling messages flowing from the core network towards to mobile station and to decipher the data and signalling messages flowing from the mobile to the core network.

In the preferred embodiment of the invention another core network or network entity may establish communication with the mobile station or vice versa while the communication with the first core network is still active. The second core network or network entity authenticates the mobile and second ciphering keys Kc2 are calculated. Then, as decribed above, the second core network generates and transmits a second message comprising the second key and data indicative of the algorithm to be used with the second key to the ciphering controller. The ciphering controller receives said second message and compares the first and second ciphering keys and the related algorithms. If the first and second ciphering keys and the related algorithms are equally reliable, the ciphering controller ciphers and deciphers data and signalling messages to and from the first and second core networks with the key and algorithm it was using already. However, if the second ciphering key and it's related algorithm provide improved encryption the ciphering center starts using the second key and it's related algorithm for the communication with the first core network as well. This will result in that ciphering control will generate and tnd transmit MS a message commanding it to act accordingly.

In another embodiment of the present invention the respective different keys are used for ciphering user data in different communications but the key and it's related algorithm with higher ciphering capabilities are used for ciphering the signalling messages to and from both core networks.

In yet another embodiment, after receiveing the message containing the second ciphering key Kc2, the ciphering control acknowledges said message

with another message containing information indicative of the selected ciphering key and algorithm.

In another embodiment, there is only one entity controlling the ciphering in CN.

In another embodiment the is an interface between the two ciphering control entites in CN providing the required coordination.

In the preferred embodiment of the present invention it is possible that the communications to the mobile station are rerouted via another serving radio network controller. Should this occur, the parameters used for ciphering and deciphering (along with other parameters required to establish the communication via the target controller) need to be transferred to the new location of the ciphering controller via CN. This is done by signallig the parameters transparently through the corresponding core networks. Alternatively this may be done by signalling the parameters over Iu interfacde between radio network controllers.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is described in more detail in the following with reference to the accompanying drawings, of which

Figure 1 is an illustration of prior art mobile communication system.

Figure 2 is an illustartion of the UMTS network of the preferred embodiment of the present invention.

Figure 3

Figure 4

Same reference numerals are used for similar entities in the figures.

DETAILED DESCRIPTION

The ciphering is likely to be done within UTRAN in UMTS[1]. In the two MM option there are two entities, i.e., MSC and SGSN, which may request ciphering in the radio interface.

It is assumed that in UMTS the ciphering key and the allowed ciphering algorithms are supplied by CN domains to the UTRAN usually in the beginning of the connection. Receipt of the ciphering command message at the UTRAN will cause the generation of a radio interface ciphering command message and, if applicable, invoke the encryption device and start data stream ciphering. The CN domain is noted if the ciphering is executed successfully in the radio interface and the selected ciphering algorithm.

When new connection is established from other CN domain, which is not having any connection to the UE, the new CN domain also supplies the ciphering key and the ciphering algorithms allowed to use to UTRAN in the beginning of the connection. This is due to the fact CN domains are independent from each other.

If it is assumed that only one ciphering key and one ciphering algorithm are used for all connections, this leads to a situation, in which there are two ciphering keys supplied from CN domains and only one of them is used.

[1] The security requirements for UMTS is still for further study.

To handle this situation, UTRAN must select either one of the ciphering keys. If there are no differences between the ciphering requirements[2] requested by two CN domains then, e.g., the first ciphering key and the algorithm is maintained (see Figure 3).

As a result of the selection of the ciphering key between two different CN domains (if both CN domains have active connection(s) to the UE) either one of the CN domains does not know the correct ciphering key used for the connection(s). Only UTRAN and UE know the correct ciphering key used.

It may be required to use one ciphering key for, e.g., one radio access bearer. Different user plane bearers are ciphered by different ciphering keys supplied by the CN domain respectly. However, in the control plane[3] only one ciphering key is used and therefore in the control plane there must be coordination between ciphering keys supplied by CN domains.

The coordination in the control plane is similar to what is presented for one ciphering key used in UTRAN option (ch. 2.1). In the control plane, UTRAN must select either one of the ciphering keys supplied from CN domains if both CN domains are active.

In GSM, when inter-BSC handover is performed, MSC sends the ciphering key and allowed algorithms to the target BSC in the BSSMAP HANDOVER REQUEST message. In GPRS, because the SGSN performs the ciphering, the inter-BSC handover does not cause any need for the ciphering key management.

---

[2] E.g. a requirement for more efficient ciphering algorithm that is currently used for the connection(s).
[3] In this case, the control plane means the RRC connection between the UE and UTRAN.

For UMTS, the GSM approach is not applicable on the serving RNC (SRNC) relocation, because CN domains do not necessary know the correct ciphering key used as it is described above.

It is recommended that the ciphering key is transferred in the transparent (to CN) UTRAN information field from the source RNC to the target RNC in the RANAP SRNC REQUIRED and RANAP SRNC REQUEST messages (see Figure 4). In this way the correct ciphering key is transferred to the target RNC.

In the handover from UMTS to GSM, the ciphering key cannot be transferred transparently like it is proposed for UMTS. The CN (or IWU) has to build the BSSMAP HO REQUEST message, having the ciphering key from the MSC. 2G-SGSN receives its ciphering key from the old 3G-SGSN via Gn-interface as it is done in GPRS.

If the ciphering keys used in UMTS are different compared to GSM, e.g., the ciphering key length is different, both MSC and SGSN ciphering keys must be changed in UMTS-GSM handover.

In GSM, the A-interface BSSMAP supports a transparent field in the BSSMAP HO REQUIRED and HO REQUEST messages, which allowes to utilize the proposed solution also GSM CN connected to the UTRAN.

In view of the foregoing description it will be evident to a person skilled in the art that various modifications may be made within the scope of the invention. While a preferred embodiment of the invention has been described in detail, it should be apparent that many modifications and variations thereto are possible, all of which fall within the true spirit and scope of the invention.

Claims

1. A mobile system
2. A method
3. A network element
4. A method of handing over

FIGURE 1

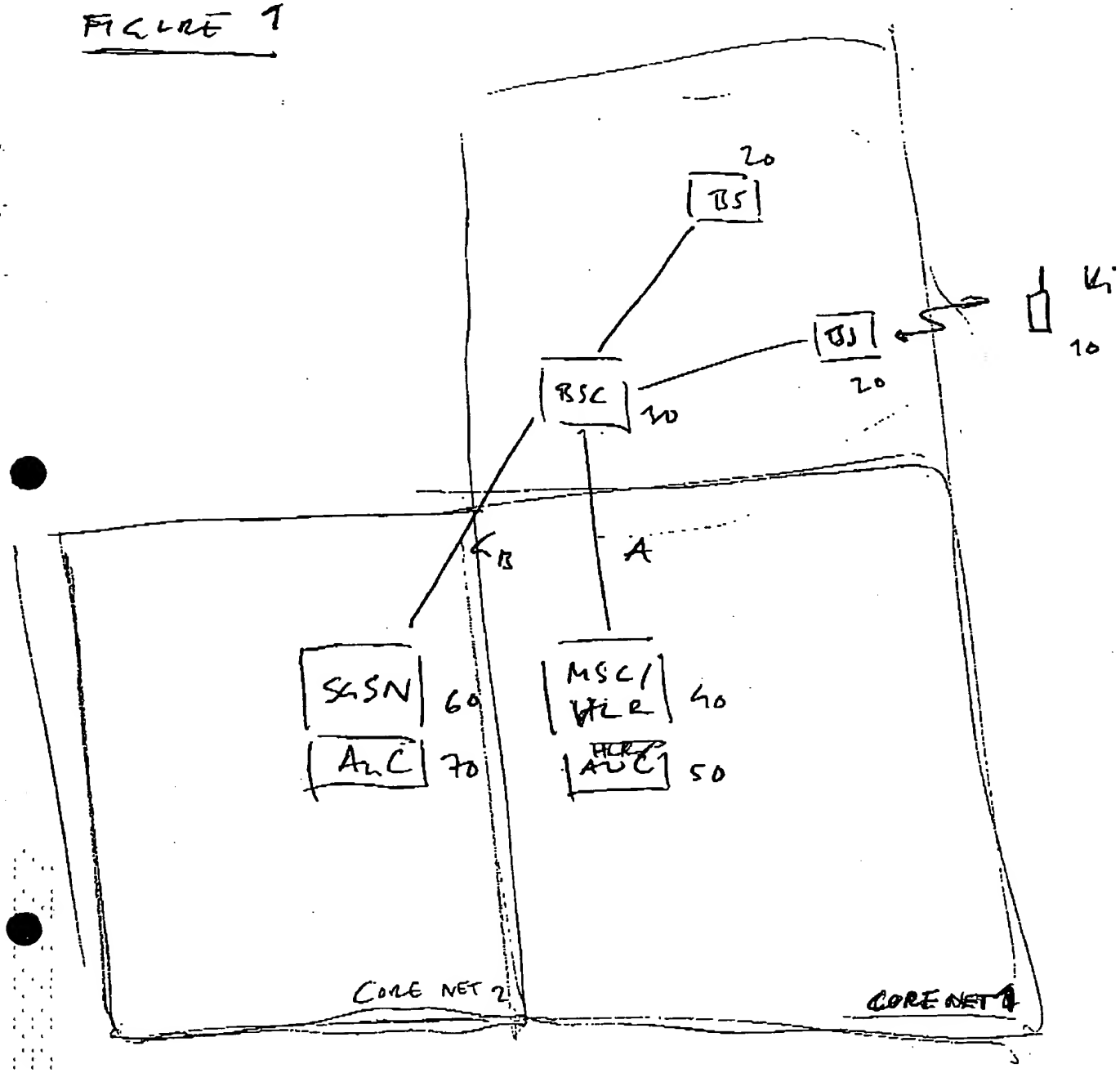
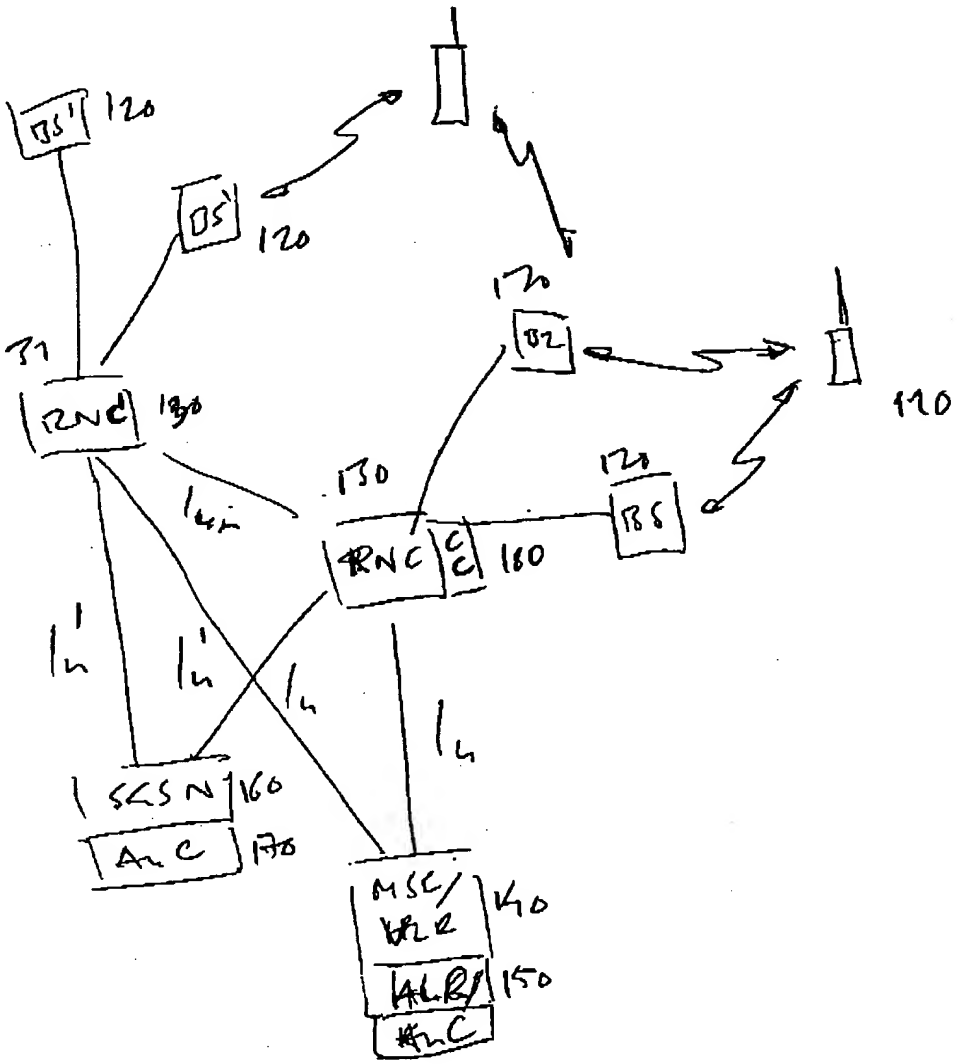

BS
20
Um
BSC
30
BS
20
10
A
B
SGSN
60
MSC/
VLR
40
GMLC
AUC
70
AUC
50
CORE NET 2
CORE NET 1

FIGURE 2



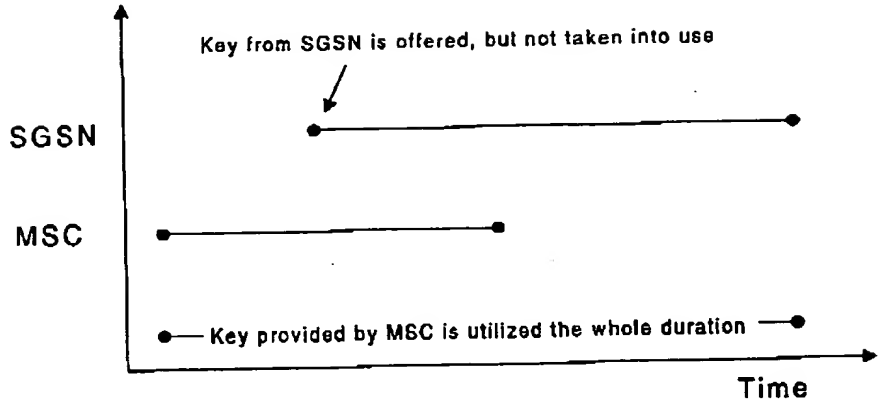


Figure 3. One ciphering key use in the UTRAN

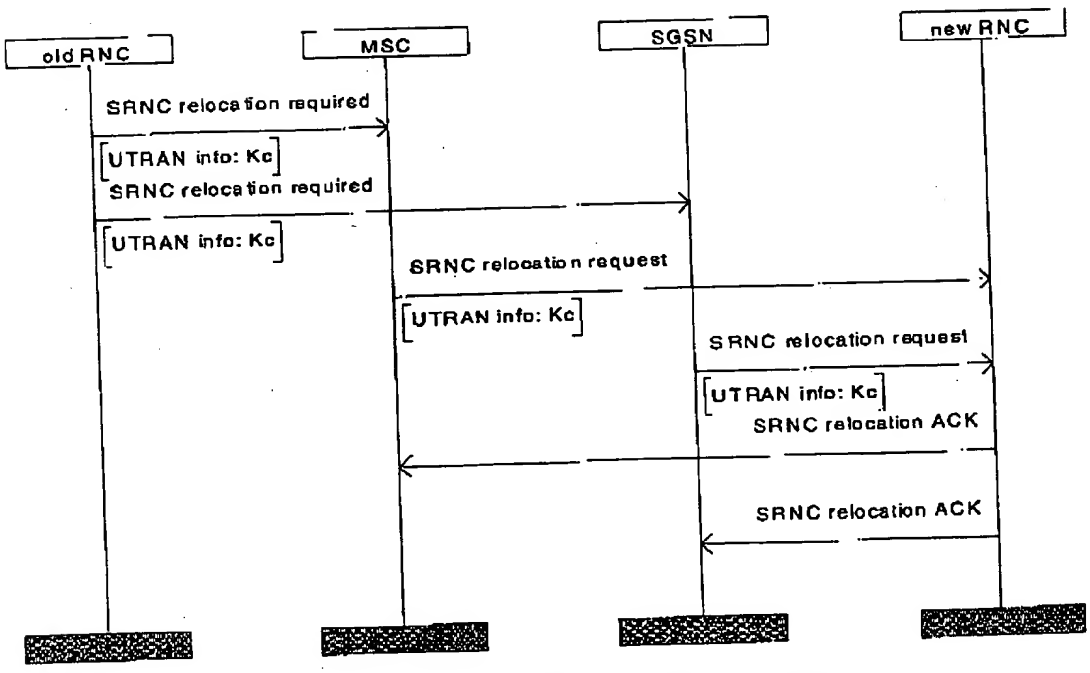


Figure 4. The ciphering key transfer in SRNC relocation procedure